Fail2ban - konfiguracija i uporaba, 1. dio

Slušajući zahtjeve kolega sistem-inženjera, u CARNetovu ponudu paketa uvrstili smo fail2ban-cn. Riječ je o jednostavnom i efikasnom sustavu zaštite koji prati logove i na određene učestale pojave blokira napadača.

Ovo čini uporabom iptables pravila, te tako blokira sve IP adrese s kojih dolaze napadi. Napadi najčešće dolaze od strane slabo upućenih korisnika, koji pokreću skripte i programe koje pronađu na Internetu (takozvani *script-kiddies*). Uspješnost provala preko ovih skripti je izuzetno niska, ali resurse utrošene s naše strane na ove napade, kao i mogućnost upada na sustav ne treba zanemariti.

Iako postoje drugi sustavi zaštite zasnovani na ovom principu, fail2ban je jedan od najjednostavnijih. On štiti odmah nakon instalacije, i ne traži više nikakvo konfiguriranje. Automatski štiti od SSH napada, iako je moguće zaštititi i druge servise bazirane na PAM-u.

Odmah ćemo se osvrnuti na mane fail2ban pristupa. Fail2ban je često kritiziran kao nepotreban servis, jer troši sistemske resurse (doduše, jako male), a ista se stvar može postići s recent mehanizmom [1] ugrađenim preko modula ipt_recent (http://www.snowman.net/projects/ipt_recent [2]) u iptablesima.

Najopasnije što se može dogoditi s fail2ban pristupom je da bilo tko na sustavu može uspješno zaustaviti rad bilo kojeg servisa krivotvorenjem unosa u logovima. Zapisati nesto u logove mogu i programski jezici, primjerice PHP, pa stoga treba pripaziti na to tko može pisati u logove. Možda bi bilo dobro zaštititi /dev/log device tako da se promijeni grupa, a sve servise potom upišemo u tu grupu.

Da ti napadi nisu rijetkost, pokazat će sljedeća naredba, odnosno niz naredbi:

```
zcat /var/log/auth.log*gz | grep 'Failed password' | grep sshd | \
      awk '{print $1,$2}' | sort | uniq -c | sort -n -k 3
```

Nakon instalacije, sustav automatski postaje aktivan i podrazumijevano je sustav zaštićen od SSH *brute force* napada. Pogledajmo te podrazumijevane vrijednosti, i lokacije konfiguracijskih datoteka.

Glavna konfiguracijska datoteka je /etc/fail2ban/fail2ban.conf. Ostale konfiguracijske datoteke se, kako je to već uobičajeno na Debianu, nalaze u conf.d direktorijima action.d, filter.d, te u dodatnoj konfiguracijskoj datoteci jail.conf. Ove konfiguracijske datoteke odražavaju interni način rada fail2ban-a:

filter - određuje što će izazvati "okidanje" akcije, uporabom regularnih izraza
action - određuje jednu ili više odgovora na "okidanje"
jail - skupina filtera i jedne (ili više) akcija

Navest ćemo primjer za SSH. U datoteci jail.conf se nalazi unos:

```
[ssh]
enabled = true
port    = ssh
```

```
filter  = sshd
logpath  = /var/log/auth.log
maxretry = 6
```

U datoteci action.d/sshd.conf možemo naići na unose poput ovoga:

```
[INCLUDES]
before = common.conf


[Definition]
_daemon = sshd

failregex = ^%(__prefix_line)s(?:error: PAM: )?Authentication failure for .* from <HO
ST>\s*$
            ^%(__prefix_line)srefused connect from \S+ \(<HOST>\)\s*$
            ^%(__prefix_line)sAddress <HOST> .* POSSIBLE BREAK-IN ATTEMPT\s*$
ignoreregex =
```

I na kraju, u datotekama akcija (podsjetimo se, može ih biti više za jedan jail) možemo naći iptables pravila. Primjerice:

```
[Definition]
actionstart = iptables -N fail2ban-<name>
              iptables -A fail2ban-<name> -j RETURN
              iptables -I INPUT -p <protocol> --dport <port> -j fail2ban-<name>

actionstop = iptables -D INPUT -p <protocol> --dport <port> -j fail2ban-<name>
             iptables -F fail2ban-<name>
             iptables -X fail2ban-<name>

actioncheck = iptables -n -L INPUT | grep -q fail2ban-<name>

actionban = iptables -I fail2ban-<name> 1 -s <ip> -j DROP

actionunban = iptables -D fail2ban-<name> -s <ip> -j DROP

[Init]
name = default
port = ssh
protocol = tcp
```

Iptables pravilima se nećemo u ovom članku baviti, samo ćemo reći da fail2ban prilikom starta pokreće akciju "actionstart", prilikom gašenja "actionstop", a i ostalim akcijama samo ime govori prilikom čega se pokreću.

- Logirajte [3] se za dodavanje komentara

uto, 2009-03-24 14:51 - Željko Boroš**Kategorije:** Software [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/544

Links
[1] https://sysportal.carnet.hr/node/71
[2] http://www.snowman.net/projects/ipt_recent
[3] https://sysportal.carnet.hr/sysportallogin
[4] https://sysportal.carnet.hr/taxonomy/term/25